Manual de segurança SIL

PolyTrans® P32000P0/1*

ThermoTrans® P32100P0/1*

SensoTrans® P32200P0/1*

SensoTrans® P32300P0/1*

www.knick.de

Knick

Índice

1 Âmbito de aplicação e padrões

Este manual de segurança aplica-se a transdutores das séries PolyTrans® P32000P0/1*, ThermoTrans® P32100P0/1*, SensoTrans® P32200P0/1* e SensoTrans® P32300P0/1*.

Versões de hardware e software válidas:

- Número de série a partir de 1657362
- Software do aparelho a partir de rev. 1.28 / 2.0

Os transdutores de segurança da série P32xxxP0/1* da Knick Elektronische Messgeräte GmbH & Co. KG estão certificados pela TÜV em conformidade com a norma EN 61508 para SIL 2 (SIL 3 em caso de arquitetura redundante):

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie (ASI)
Am Grauen Stein
D - 51105 Köln

Certificado e relatório de teste nº: 968/EZ 272.00/07

Os transdutores foram desenvolvidos e testados em conformidade com os seguintes padrões:

- **EN 61508: 2001**
  Segurança funcional de sistemas de segurança elétricos/eletrônicos/eletrônicos programáveis
- **EN 61511: 2004**
  Segurança funcional – Sistemas técnicos de segurança para a indústria de processos
- **EN 61010-1: 2001**
  Disposições de segurança para aparelhos elétricos de medição, controle, regulação e laboratório
- **EN 61326-1: 2006**
  Aparelhos elétricos de medição, controle, regulação e laboratório – Requisitos CEM
- **EN 61326-2-3: 2006**
  Aparelhos elétricos de medição, controle, regulação e laboratório – Requisitos CEM – Parte 2-3: Requisitos especiais – Disposição de teste, condições de funcionamento e características de potência para transdutores com condicionamento de sinal integrado ou independente
- **IEC 61326-3-2: 2006**
  Aparelhos elétricos de medição, controle, regulação e laboratório – Requisitos CEM – Parte 3-2: Requisitos de imunidade eletromagnética para aparelhos que realizem funções relacionadas com a segurança ou que sejam aplicados para funções de segurança (segurança funcional) – Aplicações em áreas industriais com ambiente eletromagnético especial
- **EN 50178: 1997**
  Equipamento eletrônico para uso em instalações de energia

1.1 Abreviaturas

Abreviatura	Inglês	Português
SIL	Safety Integrity Level	A norma internacional IEC 61508 define quatro Safety Integrity Level (Nível de Integridade de Segurança) independentes (SIL 1 a SIL 4). Cada nível corresponde a um intervalo de probabilidade para a falha de uma função de segurança. Quanto mais elevado o Safety Integrity Level (Nível de Integridade de Segurança) dos sistemas de segurança, mais reduzida a probabilidade de não executar as funções de segurança exigidas.
PFD	Probability of Failure on Demand	Probabilidade de falhas perigosas de uma função de segurança em caso de exigência
PFD_G	Average Probability of Failure on Demand	Probabilidade média de uma falha perigosa com exigência de um grupo de canais com comparador ou votador por maioria
PFH	Probability of a dangerous Failure per Hour	Probabilidade de falha por hora para a função de segurança
PFH_G	Average Probability of a dangerous Failure per Hour	Probabilidade de falha por hora para um grupo de canais com comparador ou votador por maioria
SFF	Safe Failure Fraction	Proporção de falhas inofensivas: proporção de falhas sem potencial de colocar o sistema de segurança em um estado de funcionamento perigoso ou não permitido
λ_S	Rate of safe failures	Taxa de falhas inofensivas por hora
λ_D	Rate of dangerous failures	Taxa de falhas perigosas por hora
λ_{DU}	Rate of dangerous undetected failures	Taxa de falhas perigosas não identificadas por hora
λ_{DD}	Rate of dangerous detected failures	Taxa de falhas perigosas identificadas por hora
DC	Diagnostic Coverage of dangerous failures	Grau de cobertura de diagnóstico: $DC = \lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$
HFT	Hardware Fault Tolerance	Tolerância de erros de hardware: capacidade de uma unidade de funcionamento de continuar a executar uma função exigida em caso de ocorrência de erros ou desvios

Abrevia-tura	**Inglês**	**Português**
MTBF	Mean Time Between Failures	Período médio entre duas falhas
MTTR	Mean Time To Repair	Período médio entre a ocorrência de um erro em um aparelho ou sistema e a sua reparação
FIT	Failure In Time	1 x 10^{-9} erros por hora
TI	Test Interval between life testing of the safety function	Intervalo de verificação entre testes de funcionamento da função de proteção
XooYD	X out of Y Voting (e.g. 1oo2)	Classificação e descrição do sistema de segurança em termos de redundância e método de seleção aplicado. "Y" indica a frequência com que a função de segurança é executada (redundância). "X" determina quantos canais devem trabalhar corretamente. Exemplo de medição de temperatura: Arquitetura 1oo2. O sistema de segurança decide que um limite de temperatura predefinido foi ultrapassado, caso um dos dois sensores de temperatura atinja este limite. Com uma arquitetura 1oo1 está disponível apenas um sensor de temperatura. "D" indica que o sistema contém uma função de diagnóstico.
t_{CE}	Channel Equivalent mean down time	Período médio de indefinição de equivalência (em horas), período total de indefinição para todos os componentes em um canal do sistema parcial
t_{GE}	Voted Group Equivalent mean down time	Período médio de indefinição de equivalência (em horas) para um grupo com comparador ou votador por maioria, período total de indefinição para todos os canais em um grupo com comparador ou votador por maioria

2 Descrição do aparelho e âmbito de aplicação

2.1 Função de segurança

Os transdutores transmitem as variáveis de entrada com separação galvânica para um sinal de saída analógico normalizado 0/4 a 20 mA ou 0 a 5/10 V. A função de transferência pode ser adaptada aos sensores ligados do lado de entrada. O sinal de saída analógico é reencaminhado para uma unidade lógica (por ex. um CLP).

Os aparelhos até SIL 2 podem ser aplicados em uma arquitetura de um canal (1oo1). Em uma arquitetura de vários canais redundante é possível a aplicação até SIL 3. Os sinais de saída dos transdutores devem ser monitorados por um dispositivo de segurança adequado superior (por ex. função de monitoramento de um CLP) como um sistema de 1 de 2 para os fins enunciados na norma DIN EN 61508 (v. DIN EN 61508-6, p.2.2.2).

2.2 Definição do estado seguro

Tipo de sinal de saída	Estado seguro
0 – 20 mA	≤ 3,6 mA ; ≥ 21 mA
4 – 20 mA	≤ 3,6 mA ; ≥ 21 mA
0 – 10 V	≤ 0,1 V ; ≥ 10,5 V
0 – 5 V	≤ 0,1 V ; ≥ 5,25 V

3 Indicações acerca do planejamento

3.1 Modo de funcionamento com taxa de exigência reduzida

Os transdutores são aplicados no modo de funcionamento com taxa de exigência reduzida (low demand mode), caso a taxa de exigência dos transdutores não seja superior a uma vez por ano e não seja mais do dobro da frequência do teste repetido (DIN EN 61508-4, 3.5.12).

O modo de funcionamento com taxa de exigência reduzida também pode ser acionado, caso a proporção da taxa de teste de diagnóstico interna do transdutor em relação à taxa de exigência ultrapasse o valor 100 (DIN EN 61508-2, 7.4.3.2.5).

O respectivo parâmetro é o valor PFD. O valor depende do intervalo de teste TI entre os testes de funcionamento da função de proteção.

3.2 Modo de funcionamento com taxa de exigência elevada

Caso não se aplique o "Modo de funcionamento com taxa de exigência reduzida", o transdutor deve ser aplicado como sistema parcial de segurança no modo de funcionamento com taxa de exigência elevada ou contínua (high demand or continuous mode) (DIN EN 61508-4, 3.5.12).

O período de tolerância de erros do sistema completo deve ser superior à soma dos tempos de reação ou dos intervalos de teste de diagnóstico de todos os componentes da cadeia de medição de segurança. O respectivo parâmetro é o valor PFH.

3.3 Tipos de erro

Uma falha inofensiva (safe failure) não tem o potencial de colocar o sistema técnico de segurança em um estado perigoso ou não funcional. O transdutor entra no estado seguro definido ou no modo de defeito, por ex. 21 mA caso ultrapassado um intervalo de medição.

Uma falha perigosa não identificada (dangerous undetected failure) tem o potencial de colocar o sistema técnico de segurança em um estado perigoso ou não funcional. O transdutor não entra em um estado seguro definido ou no modo de defeito.

3.4 Intervalo de teste de diagnóstico

Nos transdutores são executadas, a par das efetivas funções de segurança, constantes funções de diagnóstico para localizar comportamento incorreto. O intervalo de teste de diagnóstico é o período durante o qual estes testes são totalmente executados e repetidos. Dentro deste período são detectados erros de hardware ocasionais.

4 Montagem e instalação

Para os transdutores devem estar disponíveis, em função da versão, as seguintes documentações:

PolyTrans® P32000P0/1x	ThermoTrans® P32100P0/1x	SensoTrans® P32200P0/1x	SensoTrans® P32300P0/1x
Manual de instruções TA-254.111-KNxxx	Manual de instruções TA-254.113-KNxxx	Manual de instruções TA-254.114-KNxxx	Manual de instruções TA-254.115-KNxxx

As indicações, condições básicas e limites contidos nos manuais de instruções devem ser considerados durante a instalação e operação dos transdutores.

Os aparelhos com os quais é necessário um maior grau de disponibilidade devem ser atribuídos à categoria de sobretensão III. Na categoria de sobretensão III e grau de contaminação 2 é permitida uma tensão de trabalho de no máximo 150 V AC/DC. Com tensões de trabalho > 150 V AC/DC se deve assegurar, através de medidas de proteção contra sobretensão adequadas, que a categoria de sobretensão III seja atingida.

Os cabos de alimentação do sensor no ponto de medição até ao transdutor devem ser dispostos de modo que possa ser excluído um curto-circuito entre os condutores e o ambiente envolvente dos cabos.

Com a corrente do tipo de sinal de saída configurado (por ex. 4 … 20 mA) a carga de saída deve ser ≥ 50 Ω.

Antes da colocação em funcionamento ou após qualquer alteração da parametrização deve-se verificar o funcionamento devido do transdutor (ver capítulo 5.1 "Verificação do funcionamento").

Caso a parametrização seja efetuada através da interface IrDA®, o transdutor deve ser em seguida colocado em Read-Only Mode. Neste modo de funcionamento, podem ser apenas enviados dados pelo transdutor através da interface IrDA® (indicação do valor de medição, estatísticas, ...).

Ligar Read-Only Mode:

- Todos os interruptores DIP = 0
- Todos os interruptores rotativos = 0

Depois de efetuada a parametrização, os interruptores devem ser cobertos com a película de poliimido adesivo fornecida.

5 Verificações regulares

O teste de funcionamento regular se destina a localizar possíveis erros perigosos não identificados pelo autodiagnóstico. A funcionalidade do transdutor deve por isso ser verificada em intervalos adequados.

A seleção do tipo de verificação e os intervalos de tempo são da inteira responsabilidade do proprietário. Os intervalos de teste são determinados com o cálculo de cada circuito de segurança de uma instalação (valores PFD).

O teste deve ser realizado de modo que possa ser comprovado o funcionamento em perfeitas condições da função de segurança na cooperação de todos os componentes.

5.1 Verificação do funcionamento

Os valores PFD documentados no capítulo 6.x se aplicam para o intervalo de verificação TI = 1 ano. A funcionalidade do transdutor deve ser verificada na aplicação. Para tal, você deverá proceder do seguinte modo:

- O transdutor é ligado com a saída aberta (Carga = ∞). As mensagens de estado e de diagnóstico exibidas por LED devem ser verificadas:
  - Não deve ser sinalizado qualquer erro do aparelho (mensagem de erro 10).
  - Com a corrente do tipo de sinal de saída configurada (por ex. 4 … 20 mA) deverá ser sinalizada a mensagem de erro 6 (carga de erro de saída).
- Predefinir os valores nominais do início e do final do intervalo de medição bem como de um valor médio (por ex. valor 50%). Deve-se verificar se o desvio de medição se encontra dentro das tolerâncias especificadas.
- A transição para o estado seguro deve ser verificada. Esta verificação é efetuada preferencialmente pela simulação de uma ruptura do cabo (entrada aberta). De seguida, a saída regula para ≥ 21 mA (saídas de corrente) ou ≥ 5,25 V ou ≥10,5 V (saídas de tensão). É emitida uma mensagem de erro "Sensor aberto" (LED vermelho pisca 4 vezes).

O sinal de erro permanece inalterado após o final da causa de erro (mensagem de erro permanente). A mensagem de erro é reposta reiniciando (ligar/desligar energia auxiliar ou através de IrDA).

Caso o teste de funcionamento tenha um resultado negativo, o transdutor deve ser colocado fora de serviço e o processo deve ser mantido em estado seguro através de outras medidas.

O próprio transdutor não requer manutenção.

6 Parâmetros técnicos de segurança

6.1 Pressupostos

- A comunicação através da interface IrDA é utilizada exclusivamente para a configuração do aparelho ou para funções de diagnóstico, mas não para operações técnicas de segurança cruciais.
- Após a configuração (através de interruptor rotativo/DIP ou interface IrDA) é efetuado um teste de função que assegura que a função de medição executada corresponde às predefinições.
- O tempo de reparo (MTTR) após um erro do aparelho é de no máx. 72 horas.
- A temperatura média considerada ao longo de um período de tempo prolongado é de no máx. 55 °C.
- As condições ambientais correspondem a um ambiente médio industrial.
- As especificações do manual de instruções não devem ser ultrapassadas.

6.2 Parâmetros técnicos de segurança específicos

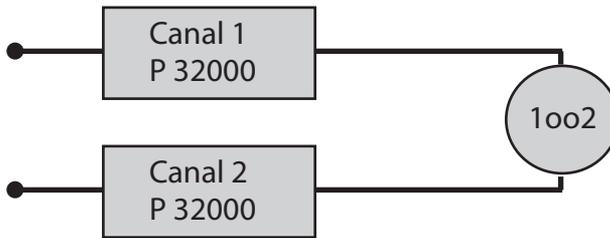
Estrutura	de 1 canal (1oo1)
Categoria	SIL 2 (Software SIL 3)
Tipo de aparelho	Tipo B
HFT	0
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
PFD_{SIL2}	$2{,}7 \cdot 10^{-4}$
PFH_{SIL2}	$4{,}8 \cdot 10^{-8}$/h
PFD_{SIL3}	$4{,}9 \cdot 10^{-6}$
PFH_{SIL3}	$8{,}5 \cdot 10^{-9}$/h
Intervalo de teste de diagnóstico	< 5 seg.
Tempo de reação de erro caso o intervalo de medição seja ultrapassado/não seja alcançado	< 2 seg.
Taxas de falha:	
λ_S	759,2 FIT
λ_D	759,2 FIT
λ_{DU}	48,1 FIT
λ_{DD}	711,1 FIT

Nota:

As taxas de falha dos componentes eletrônicos aumentam após um período de funcionamento de 8 a 12 anos, por este motivo os valores PFD e PFH resultantes se agravam (DIN EN 61508-2, 7.4.7.4, Observação 3).

6.3 Exemplo de cálculo

Como exemplo concreto de cálculo é utilizado um sistema redundante duplo com dois transdutores PolyTrans P32000® (sistema 1oo2).
O intervalo de verificação T_I é de 1 ano (8760 h).

Para que a função de segurança seja corretamente executada, os canais devem ser ligados entre si de modo que um dos canais seja suficiente para o acionamento da função de segurança. Com um sistema 1oo2 ocorre uma falha perigosa da função de segurança, caso ambos os canais funcionam simultaneamente de modo incorreto.

Equação de definição PFD para um sistema 1oo2:

$$PFD_{G,1002} = 2\,((1-\beta)\,\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\, t_{CE}\, t_{GE} + \beta_D \lambda_D MTTR + \beta \lambda_{DU} \left(\frac{T_I}{2} + MTTR\right)$$

com

$$T_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$T_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{3} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Equação de definição PFH para um sistema 1oo2:

$$PFG_{G,1002} = 2\,((1-\beta_D)\,\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\, t_{CE} + \beta_D \lambda_{DD} + \beta \lambda_{DU}$$

com

$$T_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Para este sistema resultam os seguintes valores:

Estrutura	de 2 canais (1oo2)
Categoria	SIL 3
Arquitetura	Tipo B
HFT	1
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
t_{CE}	349,5 h
t_{GE}	67,5 h
$PFD_{G,1oo2}$	$4{,}9 \cdot 10^{-6}$
$PFH_{G,1oo2}$	$8{,}5 \cdot 10^{-9}$/h

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 272.00/07

Prüfgegenstand **Product tested**	Messumformer-Reihe P32000	**Zertifikatsinhaber** **Holder of the certificate**	Knick Elektronische Messgeräte GmbH & Co. KG Beuckestrasse 22 14163 Berlin
Typbezeichnung **Type designation**	PolyTrans® P 32000 P0/1* SensoTrans® R P 32300 P0/1* SensoTrans® DMS P 32200 P0/1* ThermoTrans® P 32100 P0/1*	**Verwendungs-zweck** **Intended application**	Einsatz als Teil von Schutzein-richtungen zur Überwachung sicherheitsrelevanter Signale (Temperatur, Widerstand, Potentiometer, Spannung, ...)
Prüfgrundlagen **Codes and standards forming the basis of testing**	EN 61508:2001 EN 61511:2004 EN 61010-1:2001 EN 61326-1:2006 IEC 61326-3-2:2006 EN 50178:1997		
Prüfungsergebnis **Test results**	Die Messumformer-Reihe P32000 mit den oben genannten Typen erfüllt die gestellten Anforderungen der EN 61508 für SIL 2 bzw. SIL 3 im redundanten Betrieb und können in Schutzeinrichtungen zur Überwachung von sicherheitsrelevanten Prozessgrössen ein-gesetzt werden.		
Besondere Bedingungen **Specific requirements**	Die Sicherheitshinweise im Sicherheitshandbuch und in den Gebrauchsanleitungen der Messumformer sind zu berück-sichtigen.		

Der Prüfbericht-Nr.: 968/EZ 272.00/07 vom 12.10.2007 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Aus-weises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no.: 968/EZ 272.00/07 dated 12.10.2007 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

12.10.2007		
Datum/Date	Firmenstempel/Company Seal	Dipl.-Ing. Klaus Kemp